

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address)
 information associated with Kik username "bgillie08";)
 (fully described in Attachment A))

Case No.22-967M(NJ)

Matter No.: 2022R00300**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 2, 2022 (not to exceed 14 days)

☐ in the daytime from _____ to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

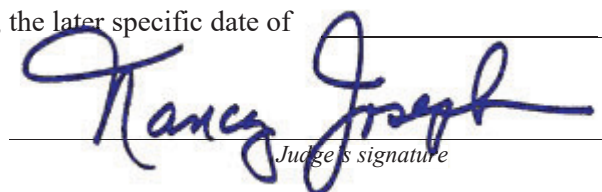
Honorable Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued 8/18/2022: @ 4:19 p.m.


 Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Kik username “**bgillic08**” that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company headquartered at 1237 7th St., Santa Monica, CA 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab, Inc is required to disclose the following information to the government for the account listed in Attachment A from **May 1, 2022 to present**:

1. All subscriber/account information, including:
 - a. Subscriber data, unrestricted by date, associated to the Kik account
 - b. Current first and last name
 - c. Email address
 - d. Phone number
 - e. Link to the most current profile picture
 - f. Device related information
 - g. Account creation date and Kik version
 - h. Birthdate and email address used to register the account
 - i. User location information
2. IP addresses associated to the Kik account, including remote port information
3. All chat logs associated to the Kik account
4. All messages sent from the Kik account to any other Kik users

5. All images and videos associated to the Kik account (to include images taken using the Kik app's camera, shared with the user's friends, or in a group chat or individual chat), including the unknown usernames and IP address associated to the sender of the images and videos and metadata associated with such images or videos
6. All other records of communications and messages made or received by the user
7. All activity logs for the account and all other documents showing the user's posts, chats, and other activities on Kik
8. A complete list of the identified Kik account's contact list and chat partners, deleted and undeleted
9. A date-stamped log showing the usernames that the Kik account added and/or blocked
10. All Kik chat groups in which the identified account is a member
11. All user-typed messages, audio notes, and video notes to friends within the Kik app using the chat feature
12. All user saved messages
13. All records of Kik searches performed by the account
14. All device-level location services maintained by Kik
15. The types of service utilized by the user
16. All abuse reports associated to the Kik account, including the unknown usernames
17. All emails associated to the Kik account

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) - transportation of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography involving the user of Kik account **bgillie08** since May 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.

3. The identity of the person(s) who communicated with the user ID about matters relating to sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 information associated with Kik username "bgillie08";
 (fully described in Attachment A)

Case No. 22-967M(NJ)
Matter No.: 2022R00300

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2256(8); § 2256 (2);	Possession, receipt or distribution of child pornography; possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct.

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)*: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

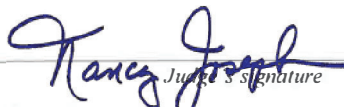
SA Daniel Gartland, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ *(specify reliable electronic means)*.

Date 8/18/2022:

City and state: Milwaukee, WI



Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
KIK ACCOUNT "**bgillie08**" THAT IS
STORED AT PREMISES CONTROLLED
BY MEDIALAB, INC., A COMPANY
HEADQUARTERED AT 1222 6TH ST.,
SANTA MONICA, CA 90401.

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., an electronic communications service provider headquartered at 1222 6th St., Santa Monica, CA 90401. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the

Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as “CSAM”).

3. Through my training and experience, I have participated in the execution of search warrants for documents and other evidence, including computers and electronic media, in cases involving crimes the FBI is authorized to investigate. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by the Attorney General to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography, the “subject offenses.” There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b) (1) (A), & (c) (1) (A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3) (A) (i).

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

- a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- d. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.
- e. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic

fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

- f. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- g. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.
- h. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- i. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- j. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.
- k. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- l. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.
- m. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

KIK MESSENGER APPLICATION INFORMATION

8. The following information comes from materials published by Kik, online research that I have conducted, from other law enforcement officers, as well as my training and experience. Kik Messenger, commonly called Kik, is an instant messaging mobile application (“app”) from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking app that permits a user to trade and disseminate various forms of digital media while using a mobile device. Kik advertised itself as “the first smartphone messenger with a built-in browser.” Kik was founded in 2009 and according to its company website was designed to “break down barriers [between operating systems] that would allow users to chat with whoever, whenever.” In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc.

9. Kik Messenger is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user selects while still within the Kik platform. Unlike some other messaging apps, Kik usernames—not phone numbers—are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers, periods, and underscores; and will never contain spaces, emoticons or special characters. MediaLab Inc. can use a Kik username to identify a Kik account to law enforcement.

10. Kik also allows users to exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users or publicly (on the Kik platform) with multiple individuals who belong to “Groups.” Groups can hold up to 50 Kik users and are oftentimes created to discuss topics such as modern popular culture-themed ideas, as well as illicit/illegal-themed ideas.

11. Kik advises that upon service of a search warrant, the company can provide the information requested in Attachment B, including: first and last name and email address provided by the user; link to the most current profile picture or background photo; device-related information; account creation date and Kik version; birthdate and email address used to register the account; user location information; the transactional chat log; the chat platform log; photographs and videos sent or received by the user for the last 30 days; the roster log; abuse reports; email events; and registration IP address associated to the username when the account was registered, including timestamp. Kik can also provide information associated with Kik groups, including group information log; group create log; group join and leave logs; group transactional chat log; group chat platform log; photographs and videos received by the group; and group abuse reports.

12. Based on my training and experience, I know Kik is often used for illegal purposes, including the receipt, distribution, and transportation of child pornography, because of the high degree of anonymity that is afforded to the user during the use of the Kik application.

IDENTIFICATION AND INVESTIGATION OF THE SUBJECT ACCOUNT

1. On May 9, 2022, the National Center for Missing and Endangered Children (NCMEC) received information from Dropbox, Inc. (Dropbox) that suspected Child Sexual Abuse Material (CSAM) was uploaded to the Dropbox account belonging to user Brandon Gilmore. The following user information was provided:

- a. Email address: thememuzickent@gmail.com
- b. Screen/username: Brandon Gilmore

2. Dropbox provided six videos uploaded to the account associated with user Brandon Gilmore. NCMEC provided the information to the Federal Bureau of Investigation for further

action. The first video showed a female removing her clothes and touching her vagina. The video then showed an adult male touch her vagina and engaged in vaginal and anal sex with the female. The female appeared to be in the early stages of puberty with minor breast development and some pubic hair. The second video showed adult male engaged in vaginal sex with a minor female. The female appeared to be pre-pubescent, lacking pubic hair and breast development. The third video showed an adult male engaged in oral sex with a minor female. The female wore a blindfold over her eyes. The words, “suck cock cum slut” were written on the blindfold. The female had facial features consistent with a pre-pubescent child. The fourth video showed a close-up view of an adult male engaged in vaginal sex with a pre-pubescent female, lacking pubic hair. The fifth video depicted an adult male laying on a bed while two unclothed females removed his pants and touched his penis and testicles. The females appeared to be pre-pubescent, lacking breast development and pubic hair. The sixth video showed a female sitting on a chair with her pants pulled down. An adult male then lifted her legs displaying her anus and vagina. The video then showed the male spreading open the minor female’s vagina. The female appeared to be pre-pubescent, lacking breast development and pubic hair. The female also wore a t-shirt with a cartoon drawing of a smiling sun. An upload log provided by Dropbox indicated the videos were uploaded on or about May 7, 2022.

3. On June 6, 2022, Dropbox provided information in response to a subpoena requesting user account information and IP addresses associated with the Dropbox user Brandon Gilmore. The information revealed that the account was accessed by IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e on May 7, 2022.

4. Further investigation determined that the IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e was assigned to an AT&T account with the following

subscriber information:

- i. Account Number: 314010876
- ii. Subscriber Name: Brianna Roeck
- iii. Account Creation: 06/11/2021
- iv. Service Address: 3640 South 87th Street, Milwaukee, WI, 53228

5. A search of law enforcement databases revealed that in June of 2021 Brandon Gilmore (XX/XX/1989) was involved in a vehicular accident in Milwaukee, WI, while driving a black Chevrolet Equinox bearing Wisconsin registration plate ACS-3373 (hereinafter “Equinox”). The registered owner of the Equinox was Brianna Roeck. Gilmore also owns a blue 2004 Chevrolet Impala registered with the state of Wisconsin at the address 3640 South 87th Street, Milwaukee, WI.

6. On July 25, 2022, Special Agents with the Federal Bureau of Investigation (FBI) observed Brianna Roeck arrive at 3640 South 87th Street, Milwaukee, WI, driving the Equinox. Agents observed Gilmore leave the address and return while driving the Equinox. Agents also observed a blue Impala without visible plate parked at the address.

7. An open-source search of Facebook revealed a profile with the name, “Brianna Röck.” The profile includes references to the “Gilmore’s” and includes photos that appear to show Brianna Roeck and Brandon Gilmore together. The profile also contains references to Brynlee Gilmore, a baby born in early-October 2021 and photos of two other female children. Based upon the information in the Facebook profile, I believe Brianna Roeck and Brandon Gilmore are in a relationship.

8. A search of law enforcement databases revealed that Brandon Gilmore is a registered sex offender and resides at the address 3640 South 87th Street, Milwaukee, WI. On July

23, 2013, Gilmore was arrested by the FBI in Minneapolis, MN for a violation of Title 18 U.S.C. § 2423 (d) and (e) Conspiracy to Facilitate in Transportation of Minors for Prostitution. The arrest was the result of an investigation into Gilmore and two other females for the transportation of a 14-year-old female from Milwaukee, WI to Bloomington, MN for the purpose of engaging in prostitution. Gilmore plead guilty to the charge and was sentenced to 82 months in federal prison and 60 months of supervised release. Gilmore remained on supervision with the United States Probation Office for the Eastern District of Wisconsin as of July 26, 2022 and was due to complete his supervision on August 13, 2024.

9. On July 27, 2022, a search warrant, issued in the United States District Court for the Eastern District of Wisconsin on July 27, 2022, was executed by the FBI at 3640 South 87th Street, Milwaukee, WI. During the search, law enforcement officers seized as evidence an Apple iPhone 13 with serial number: DPQ00N306, (hereinafter, “the Phone”) from the location. Pursuant to the search warrant, a forensic examination of the phone. The was assigned telephone number 414-708-5314 and had an Apple ID associated with the e-mail address, thememuzickent@gmail.com.

10. The Phone appeared to have an initial power on date of June 26, 2022. The phone included data from dates prior to the initial power on date. Based on my training and experience, I believe the user of the phone obtained a new device on or about June 26, 2022, and synced the Phone with data maintained in on an external cloud-based server.

11. The phone contained several social media accounts and associated conversations. A Facebook profile and Facebook Messenger account on the phone was associated with the username Charles Palmer with the identification number 10006618555099. A Kik messenger account with a username of “**bgillie08**” and the e-mail address, Ovathatop01@gmail.com. The

Apple wallet for the Phone was associated with “Brandon Gilmore” at the address 4597 North Houston Avenue, Milwaukee, WI. Law enforcement databases indicate that 4597 North Houston Avenue, Milwaukee, WI is the address of Tequila Matthews, mother of Brandon Gilmore.

12. Investigators conducted a review of Kik messenger conversations recovered from the telephone. At least two conversations contained discussions of Child Sexual Abuse Material (CSAM). On July 17, 2022, Kik user “claraoglyta_cb5” (hereinafter, “CB5”) initiated a conversation with the account associated with the phone. CB5 asked “Are you a buyer of cp mega link and video?” CB5 further provided an apparent list of the types of CSAM available. Bgillie08 responded “Samples.” A link to at least one video of suspect CSAM was sent to Bgillie08 and a request for payment was made. On July 25, 2022, **Bgillie08** messaged “Samples” to Claraoglyta_cb5, though the message did not appear to be delivered.

13. A Kik conversation between **bgillie08** and dirtydaughter101_n1k (hereinafter, “N1K”) occurred from July 17, 2022 to July 25, 2022. The conversation began with N1K sending links of known or suspected CSAM to **Bgillie08** and a request to “Send me the screenshot baby.” Bgillie08 responds with a screenshot of a \$50 payment via an electronic funds transfer application to a user named “Malacia Hyche.” **Bgillie08** then messages, “Penetration and cum” and “And anal.” N1K then provided additional videos. **Bgillie08** later states, “I’ll send more money when I have all 50 videos u promised for the 30 I sent.” After receiving a series of videos, **Bgillie08** states, “That’s not cp. That don’t count.” Further videos and requests for money were sent from N1K until July 19, 2022. On July 25, 2022, the conversation ended with **Bgillie08** asking, “Samples?”

14. Investigators conducted a review of the images and videos recovered from the Phone. The phone contained numerous selfie-style images of Brandon Gilmore, including metadata with a location in the area of 3640 South 87th Street, Milwaukee, WI. The phone

contained approximately 34 videos of known or suspected CSAM. Five of these videos are further described as follows:

- A close-up video of an infant, approximately less than one year of age, with a white fabric background. The child did not appear to have developed lower teeth. The child's bare chest was visible in the video. The child appeared to be Caucasian, though hair color and sex of the child could not be determined based upon the view of the camera. An erect adult penis was inserted into the child's mouth during the video. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately four to eight years of age, laying on her back with her legs held up. The female had short dark brown or black hair and a light skin tone. The child did not have developed breasts or pubic hair. The child's mannerisms were consistent with a mental handicap. Written on the inner thigh of the child's left leg is the letter "I", a drawing of a heart and an illegible word. The female child was completely naked, and her anus and vagina were clearly visible. There was apparent male ejaculate on the child's legs, vagina and seeping from her anus. A white-skinned adult hand with manicured fingernails pointed to the ejaculate in the child's anus. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately five to nine years of age, visible from the mid-torso down. The child was light skinned. Her face and hair were not visible in the video. The female was wearing a pink and white striped bathing suit with a pink and blue flowers or starfish pattern. The child's bathing suit was pushed to the side and her vagina was partially visible. A white skinned adult male penis

had vaginal sex with the child. The adult male's right hand was pressed down on the child's stomach area. The video appeared to have been recovered from applications on the Phone.

- A video of a pre-pubescent female, approximately five to nine years of age, standing in front of a white skinned adult male. The female child is light skinned with short brown hair. The female was wearing a white T-shirt and did not appear to be clothed from the waist down. The female did not appear to have developed breasts. The adult male was wearing a white T-shirt pulled up above his belly button. The adult male has the child perform oral sex on him. The adult male had one hand on the child's shoulder and the other hand manipulated a the zoom on a camera with a remote. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately two to six years of age, lying on a carpeted floor. The child was light skinned. The child did not have pubic hair. Her face and hair were not visible in the video. The child appeared to be wearing a green T-shirt, pulled up above her chest. The child's vagina was clearly visible in the video. A dark-skinned adult male with an erect penis had anal and vaginal sex with the child before ejaculating on the child's pubic area. The adult male held the child down at various points in the video by gripping the child's waist. The video appeared to have been recovered from applications on the Phone.

15. On July 27, 2022, Brandon Gilmore was interviewed by Special Agents of the FBI in a non-custodial setting at the FBI Milwaukee Field Office. During the interview, Gilmore stated that he had a Dropbox account when he was first released from prison. The account was registered

with the e-mail address thememuzickent@gmail.com. Gilmore maintained a few self-developed rap songs on the account and had not used it in several years. Gilmore also used the e-mail address ovathatop01@gmail.com. Gilmore provided the pass code to his phone and stated that he did not have Dropbox on the phone. He further stated that there was not child pornography on his phone. Gilmore stated he “was not concerned about child pornography” and “did not watch child pornography.”

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. This warrant is being sought under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require MediaLab, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

14. Based on the forgoing, I request that the Court issue the proposed search warrant.

15. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

16. The government will execute this warrant by serving the warrant on MediaLab, Inc. Because the warrant will be served on MediaLab, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Kik username “**bgillic08**” that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company headquartered at 1237 7th St., Santa Monica, CA 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab, Inc is required to disclose the following information to the government for the account listed in Attachment A from **May 1, 2022 to present**:

1. All subscriber/account information, including:
 - a. Subscriber data, unrestricted by date, associated to the Kik account
 - b. Current first and last name
 - c. Email address
 - d. Phone number
 - e. Link to the most current profile picture
 - f. Device related information
 - g. Account creation date and Kik version
 - h. Birthdate and email address used to register the account
 - i. User location information
2. IP addresses associated to the Kik account, including remote port information
3. All chat logs associated to the Kik account
4. All messages sent from the Kik account to any other Kik users

5. All images and videos associated to the Kik account (to include images taken using the Kik app's camera, shared with the user's friends, or in a group chat or individual chat), including the unknown usernames and IP address associated to the sender of the images and videos and metadata associated with such images or videos
6. All other records of communications and messages made or received by the user
7. All activity logs for the account and all other documents showing the user's posts, chats, and other activities on Kik
8. A complete list of the identified Kik account's contact list and chat partners, deleted and undeleted
9. A date-stamped log showing the usernames that the Kik account added and/or blocked
10. All Kik chat groups in which the identified account is a member
11. All user-typed messages, audio notes, and video notes to friends within the Kik app using the chat feature
12. All user saved messages
13. All records of Kik searches performed by the account
14. All device-level location services maintained by Kik
15. The types of service utilized by the user
16. All abuse reports associated to the Kik account, including the unknown usernames
17. All emails associated to the Kik account

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) - transportation of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography involving the user of Kik account **bgillie08** since May 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person.

3. The identity of the person(s) who communicated with the user ID about matters relating to sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.